multos
international

MULTOS M5

Securing Connected Devices

The MULTOS M5 family is a programmable, highly secure solution for embedded systems that are connected to the internet across a variety of market sectors, in the so-called Internet of Things (IoT).

As devices become smarter and more interconnected, there is a greater need to ensure those devices have the right level of security designed in. Any device connected to a digital network is open to attack, with examples of poor security practices being exploited on a daily basis. Many of these devices or system components suffer from implementation issues that are either not known during the development stages or are poorly designed in the first place. Using proven MULTOS high-security technology that has been honed over 20 years of successful smartcard projects, with over 1 billion devices deployed, we are turning those smart connected devices from merely being connected, to devices that are secure, easily provisioned, and able to be managed in the field with flexibility that is unmatched in the industry.

The MULTOS M5 family is an advanced implementation of the MULTOS operating system developed on a secure hardware chip, that provides a security solution that allows for programmable functionality (via applications loaded onto the MULTOS device), or via several built-in standard functions.

End Use Applications

MULTOS technology is ideally suited to the security demands of many sectors that utilise an embedded connected device, especially:

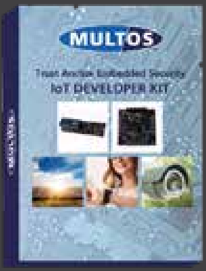
- Protecting critical assets connected via a distributed operating environment (such as the internet)
- Managing devices in the field, interacting with a central server system
- End-to-end security with distributed key management, utilising the MULTOS M5 component in the end device as the core "Trust Anchor"

Typical sectors that need a secure solution include:

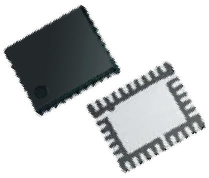
- Industrial systems
- Medical electronics
- Smart homes

Developers Kit

An evaluation & developer kit is available that contains 2 MULTOS ML5 chips and sample software.



MULTOS M5



Platform Features

MULTOS M5-P22	
MULTOS OS	MULTOS 4.5.3
Application cryptography	RNG, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, DES, 3DES, AES, SEED, RSA (up to 4096 bit keys), ECC (up to 521 bit curves)
GPIO interface	Up to 12 GPIO pins each configurable as an input or output with optional "startup" pins
Serial IO interface	Two transmit/receive serial ports up to 57,600 baud
SPI interface	Single master port, up to eight slaves
I2C interface	Single master and slave port
Contact smartcard mode	Operates as a standard MULTOS contact smartcard (ISO7816). T=0, T=1, up to 447k
Contactless smartcard mode	Operates as a standard MULTOS contactless smartcard (ISO14443). Type A, Type B, up to 848k, Mifare Classic (single 1K or 4K)
Reset pin	Reset pin for chip reset
Delays	Delay feature with optional jitter
Timers	Eight count-up and eight count-down timers
Embedded mode	Operates as a stand-alone embedded controller powered from an external supply, processes system events. Exit to MULTOS and Restart supported in embedded mode.
Combined mode	Operates as a standard MULTOS contactless smartcard powered from an external supply
Command mode	Operates as a stand-alone embedded controller powered from an external supply processing commands sent over one of the serial IO ports or over I2C
System events in embedded	Start-up, count-down timer expired, GPIO pin change, serial IO data received, I2C slave message
Free NVM for applications	At least 250K
Application replacement	Ability to replace applications with a single ALC, new application can inherit data from the replaced application
Embedded low power mode	Optional, to reduce the SLE78's power consumption when idle (low power (3mA) and ultra-low power (50uA))
Multiple power domains	Separate Vcc, GPIO and ISO power domains that support ultra-low power mode when using the ISO 14443 interface.
Security countermeasures	Extensive hardware and software security countermeasures to help protect application code and data
EMV payment applications*	M/Chip Advance R3, VSDC R5, Amex R3, D-PAS R3, PURE R2, M/Chip 4, Flash R3
Package options	SMD VQFN-32-13; Wafer (sawn)

*Notes: Specifications and functionality may change please check for availability. * Check for available configuration options*